IBM Security

How to Pen Test an ATM

BREAKING INTO NETWORK-CONNECTED BOXES OF CASH

IBM

Who am I?

- Daniel Crowley
- Research Baron at X-Force Red
- Pen tester since 2004
- Locksport enthusiast and past competition winner
- Actually holds the title of Baron (in Sealand)

Why ATMs?

- Cash-filled safe
- Windows box
- Combination cash-filled safe and Windows box
- Requires WAN connection
- Always on
- Always logged in
- Available to the public

Components of an ATM

Interface

Dispenser

Beauty Door

Computer

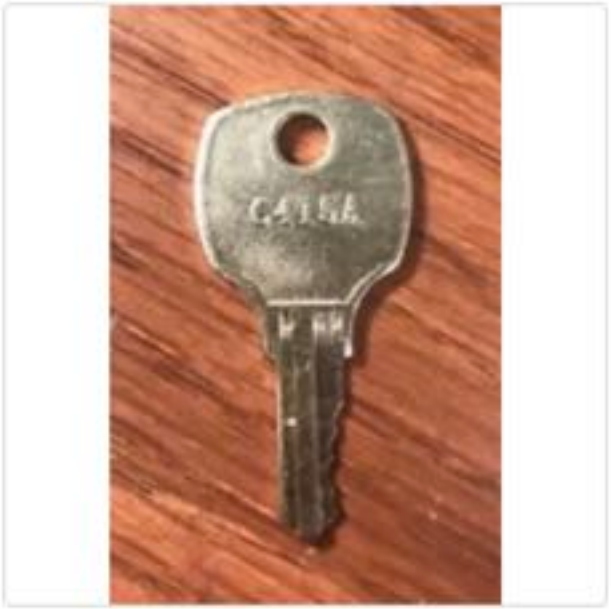
Safe

PHYSICAL

Locks

- Crap default wafer locks
- Crap default tubular locks
- Small number of possible default keys
- Lock mechanisms independent of tumbler state
- Alternative entry points

Default keys



Hantle GenMega ATM Machine N

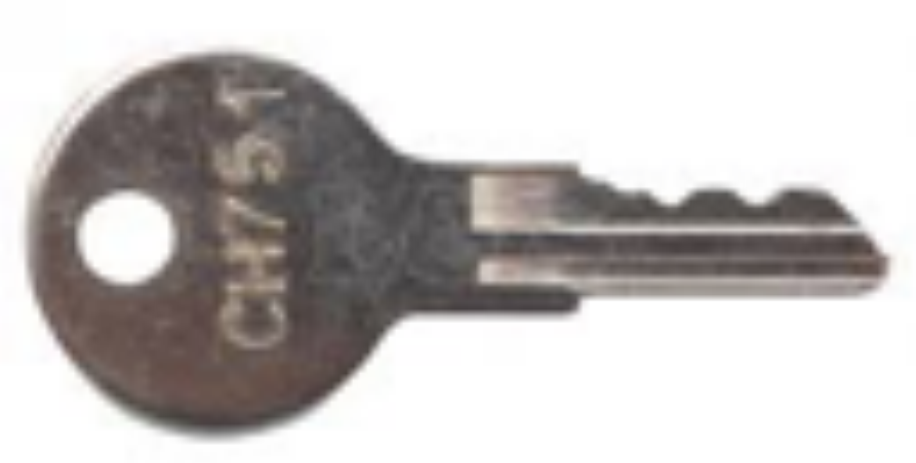
You are considering a new Hantle/Genme
G2500 and Onyx GT3000.

$7.99

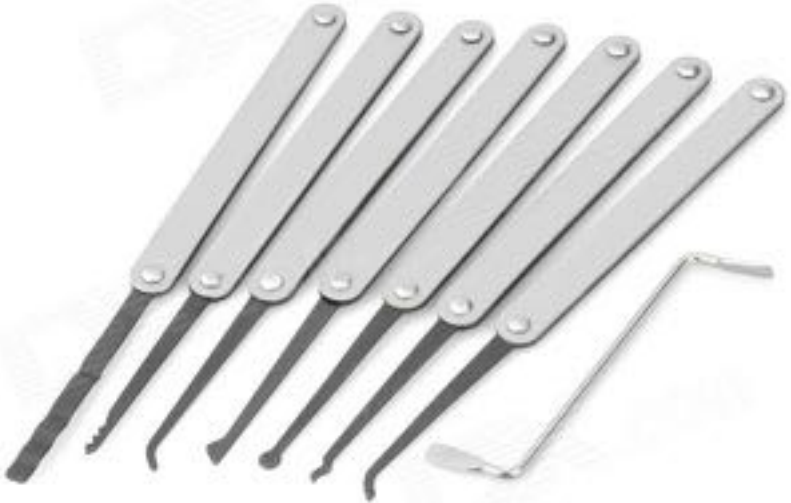
$3.00 shipping

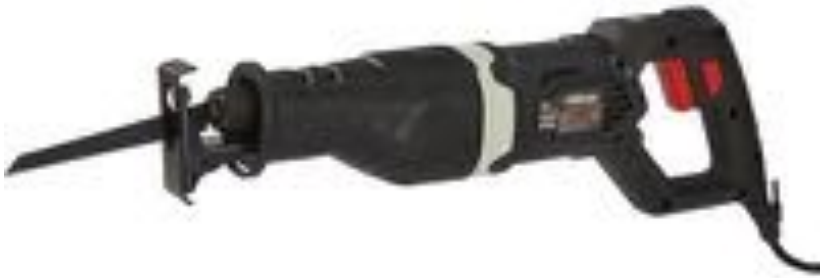
2 new & refurbished from $7.99

CH751

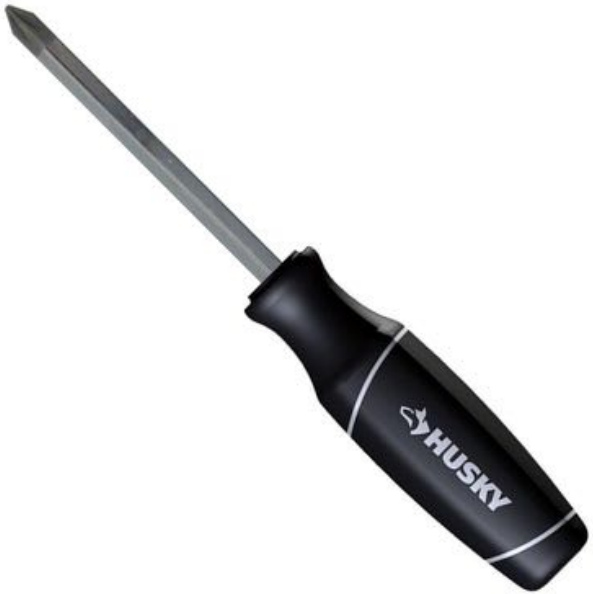


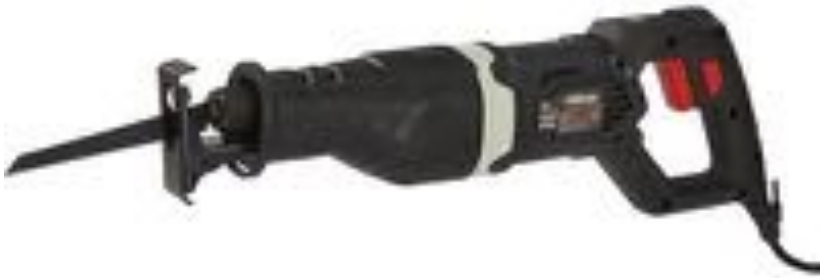
Which would win?





Which would win?





Safe

- Default entry code
- Holes
  - Dispenser
  - Power cabling
  - Network cabling
  - Serial cabling

Assorted tomfoolery

- Optical bill sensor
- Direct actuation of dispenser motors
- Hardware hax
  - JTAG/UART
  - SPI flashing

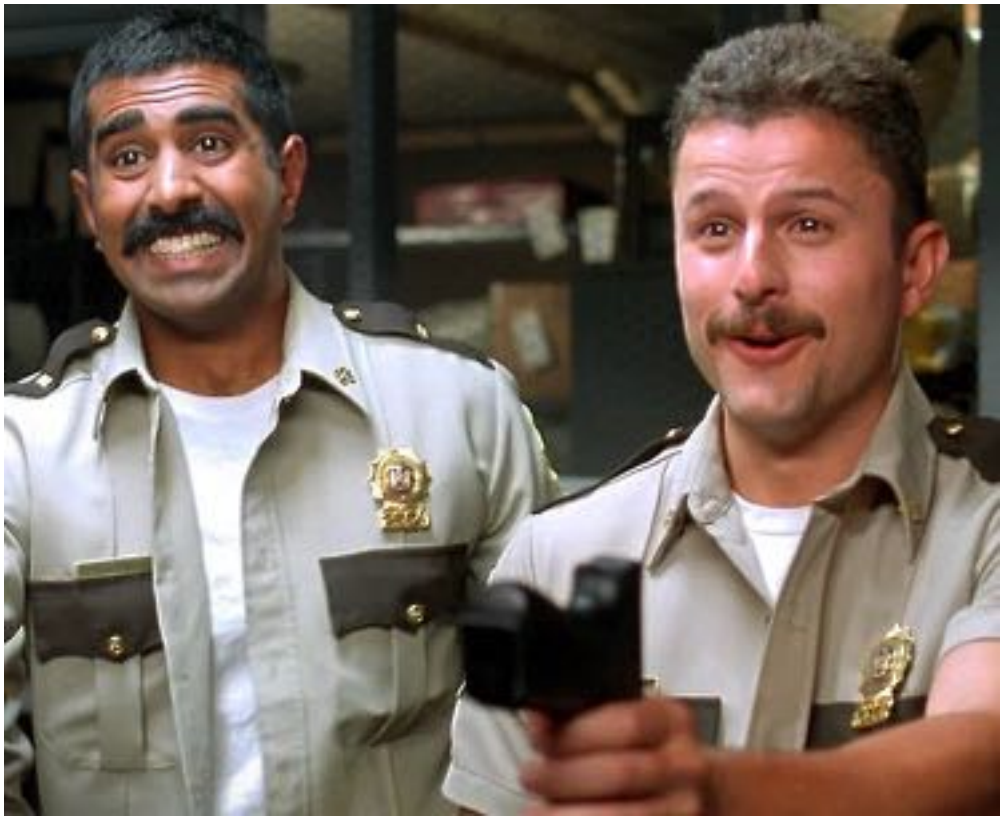
NETWORK

Encryption

- No encryption
- Fixed encryption key
- Replay attacks
- Limitations of mainframe (yes, mainframe) processing power

Exposed network gear

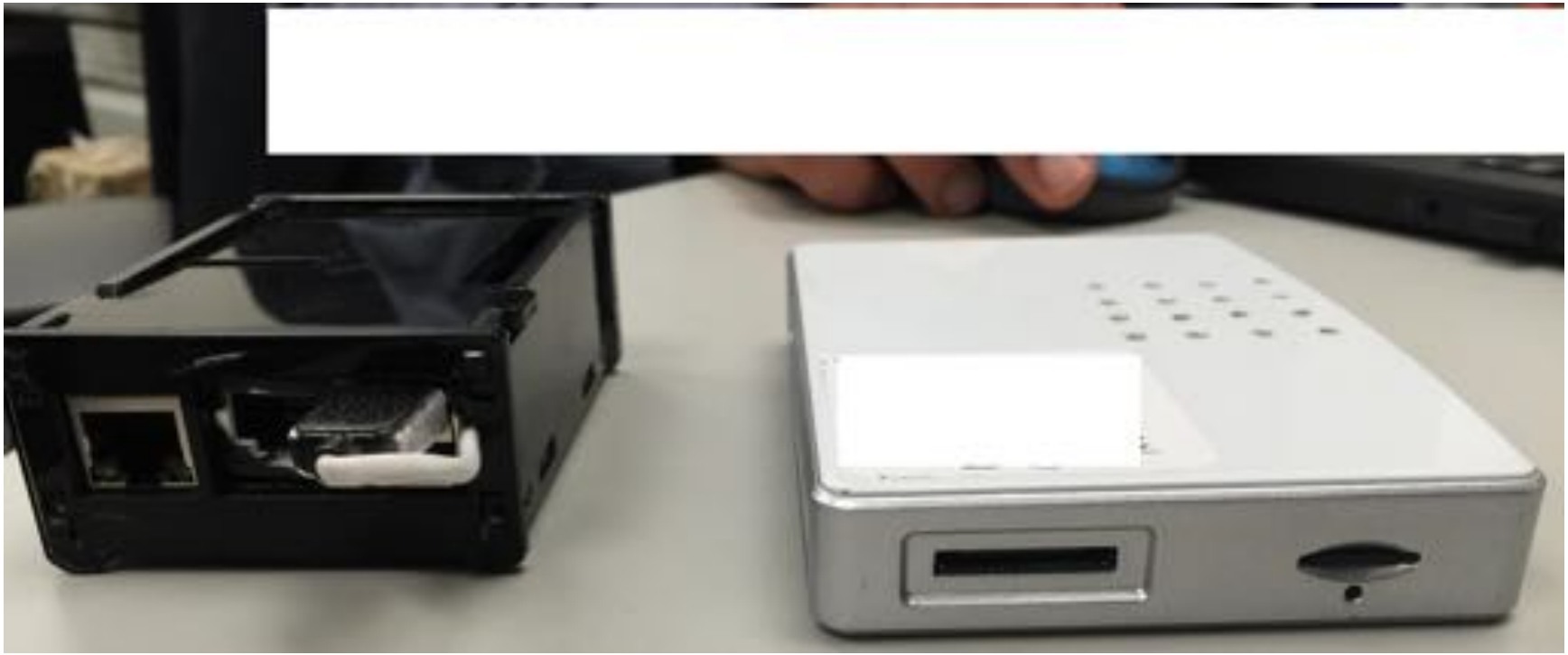
Usual network shenanigans



ATM networks

- Modems (wired or cellular)
- Ethernet
- Compromising one may allow lateral attacks
  - ...or attacks against ATM infrastructure

Real world attack



APPLICATION

Management applications

- Casino ATMs
  - Gaming server
  - Voucher scanner
- Remote management

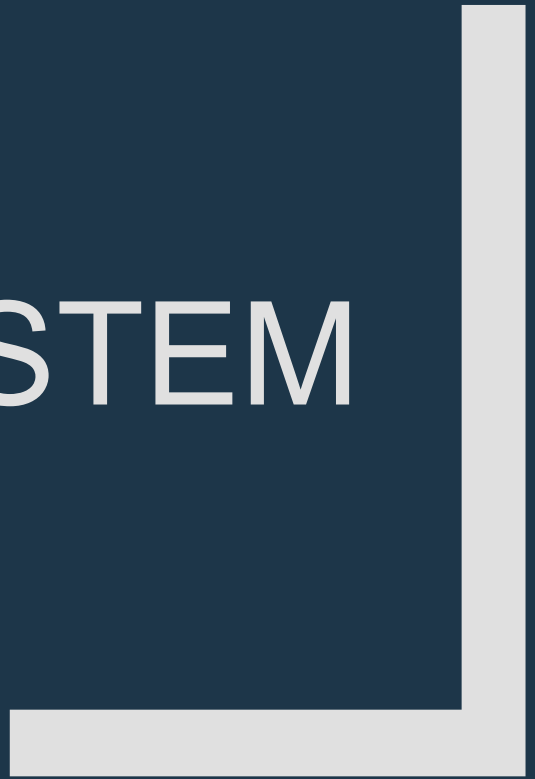
Kiosk application

- Kiosk breakout
  - Power up time
  - Touching randomly around the screen
- Management mode
  - Enter+clear+cancel, 1, 2, 3
  - Default codes
    - Any digit * 6
    - 123456
  - Management card

Network comms attack surface

- Open ports aren’t the final word!

OPERATING SYSTEM



Old OS versions

- MS08-067
- MS17-010

Misconfiguration

- NBNS/LLMNR
- WPAD
- Unencrypted hard drive

Passwords

- Weak or default passwords
- Same local admin passwords across multiple ATMs

Hotkeys

- Alt+Tab
- Win+Tab
- Ctrl+Alt+Del
- Win+E
- Win+D
- etc

DANIEL.CROWLEY1@IBM.COM

QUESTIONS?

IBM Security

estions

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

IBM